AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

THE FALLACY OF ATTRIBUTION TO ACHIEVE DETERRENCE IN CYBERSPACE

by

Robert J. Johnson, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisor: Wing Commander Graem M. Corfield

Maxwell Air Force Base, Alabama

April 2015

Disclaimer

Table of Contents

Introduction

The ability to determine the responsible party of a military attack and convince a would-be attacker that one has the ability to determine this culpability constitutes a key capability for nations wishing to deter aggression. However, within domain of cyberspace, a belligerent state, non-state and/or criminal actor can manipulate elements of the domain to shroud and/or maliciously redirect culpability elsewhere. In such an environment, is the basic premise of deterrence (threat of retaliation or denial of benefits to the attacker) still viable? This research paper will look at the problem of attribution from both a technical and national policy standpoint. Specifically, the research will briefly describe the technical problems challenging attribution and review some of the proposed solutions. Further, the research will examine the problem of attribution from a national policy standpoint to outline the potential policy solutions that could provide alternate solutions outside or in addition to the purely technical ones as well as highlight consequences of some of the proposed solutions.

This paper argues that a central focus on attack attribution to enable a retaliatory response as a means to accomplish deterrence presents an untenable, unsustainable strategy. Cyberspace, unlike other domains of air, space, land and sea, provide the ability to recreate the domain at will to complicate an attacker's ability to penetrate. This paper argues that old ideas of centralization and hardening for defense should give way to ideas of randomly moving cyber attack surfaces (logically defined vice physically defined) in order to rebalance the current asymmetry between attacker and defender. Transformative security in cyberspace can only take place when industrial age ideas are supplanted by modern information age ideas that exploit the strengths of the malleable cyber domain to ensure security. Defenders should turn the advantages that favor the offense on its head and make them the advantages of the defense. Specifically, by

complicating the cyber attack surface via ambiguity/misdirection (just as an attacker does to hide his/her identity) costs of penetrating are increased and deterrence can be enhanced with the credible prospect of a denial of benefits to the attacker. This does not mean one should abandon all efforts at attribution, but a focus of complicating the attack surface can complement attribution efforts by reducing the number of successful attacks. Thus, cyber security can be more sustainable through increased focus on resilience and denial versus detection, attribution and retaliation (after which an attack has already happened and losses have occurred). The initial sections of this research provide the preliminary analysis groundwork by detailing definitions of terms, outlining the research scope and describing the context. Prior to arguing for the need to complicate the attack surface, the paper will investigate the current attribution problem and proposed solutions.

Levels of Attribution and Types of Cyber Attacks

Before proceeding further, levels of attribution must be defined. Attribution can mean the "owner of the machine (e.g. the Enron Corporation), the physical location of the machine (e.g. Houston, Estonia, China) or the individual who is actually responsible for the attack actions."[1] Similarly, Cohen and Narayanaswamy identify four levels of attribution[2]:

1. Identification of the specific hosts (machines) involved in the attack
2. Identification of the controlling host (machine)
3. Identification of the actual human actor(s)
4. Identification of the higher organization with a specific purpose to the attack

This definition of attribution motivates the question, which level of attribution is necessary as a function of different types and/or severity of attacks? Thus, types of cyberspace attacks must be discussed to further outline the problem space.

Robert Knake parses cyberspace attacks into three categories: internet-based attacks, non-internet based attacks and supply chain threats. Non-internet based attacks refer to attacks on

systems not connected to the Internet "through other delivery mechanisms including thumb drives, CDs/DVDs, microwave or other radio transmissions."[3] Supply chain attacks include those where an actor inserts malicious software or hardware into the logistics supply chain of systems. Both non-internet based attacks and supply chain attacks can target closed network systems such as those associated with military and industrial systems. Supply chain and non-internet based attacks are described by Knake as potentially the most dangerous forms of cyberspace attack. However, attribution for these forms of attack "is no different from a traditional investigative challenge to identify the opportunity and the motive for inserting the malicious content."[4] While not necessarily the most dangerous avenue of attack, the one that poses the more difficult attribution challenge arises from internet based attacks. Knake describes these attacks as

> "difficult to deter because of the underlying architecture of the Internet, the lack of security on many hosts, and because individuals carrying out these attacks can do so remotely, from safe confines of a non-cooperative country."[5]

Within internet-based attacks, Knake further subdivides levels of attack (from most to least dangerous) as cyber war (catastrophic destructive/disruptive attacks on nation state finance, infrastructure, military networks, etc…), network exploitation (espionage), crime (profit motivated), brute force (distributed denial of service) and nuisance.[6] Now that the levels of attack from the Internet have been delineated, one particularly challenging attack approach with respect to attribution (multi-stage/multi-jurisdictional) will be described.

Internet based multi-stage attacks generally refer to the situation where an attacker on a computer infiltrates another computer or multiple computers with code designed to use those infiltrated computers as the delivery computers of an attack on an intended target. In between the attacker's source computer and the attacking computers may be a set of computers used by

the attacker as command and control (C2) computers that directly control the attacking computers.[7] This C2 layer provides the ability for the attacker to direct the attack system from a location other than his/her own system. Ultimately, multi-stage attack architectures give the attacker the advantage of redirecting the source of the attack away from his or herself. The computers infiltrated may lie within another jurisdiction than the attacker, and the target may lay within yet another jurisdiction as well, hence the term multi-jurisdictional. Here the attacker may intend to choose a nation with weak monitoring/investigative capability, weak law enforcement and/or a nation hostile to his or her intended target nation to further complicate investigation cooperation between the target nation and the nation where the attacks emanated.[8] From a policy standpoint, should the United States hold the victimized nation whose systems were compromised by the attacker as an additional culpable party? Both Yannakogeorgos and Knake make such an argument to incentivize investigation cooperation between nations as well as strengthen their cyber security and law enforcement.[9] This research will delve further into this view point and its consequences as well as analyze alternative views that disagree with this policy prescription. Before investigating these and other potential policy options as well as the appropriate level of attribution per attack type, the research must first outline its limited scope. A brief description of the basic structure of the Internet will follow to provide the proper context for the attribution problem.

Research Scope

In order to narrow the scope of the research effort, technical and policy options in this paper will only address internet-based attacks emanating from an attacker using a multi-stage, multi-jurisdictional approach. Multiple authors in cyber security describe this type of threat as the most serious problem to be addressed.[10] The paper will deal with attacks along this multi-

stage, multi-jurisdictional approach where the intent is either cyber war, espionage or crime. Distributed denial of service and nuisance internet-based attacks will not be addressed.

Structure of the Internet Complicating Attribution

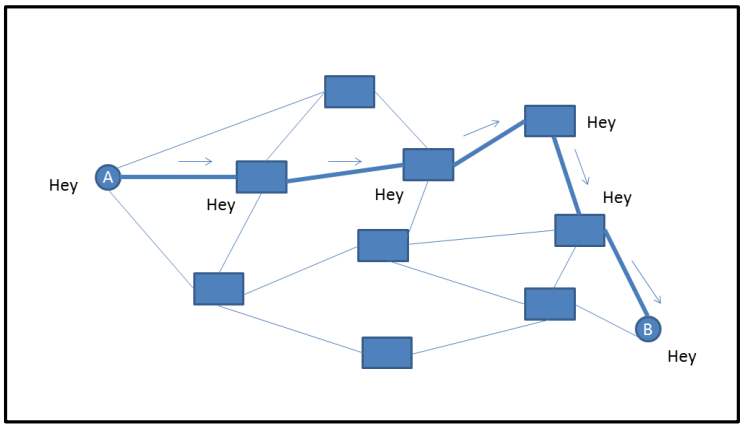
Circuit-Switched versus Packet-Switched Networks

Information passed from one entity to another via some route describes the basic idea of a network.

> "In a circuit-switched network, before an exchange of information occurs between two nodes, a (dedicated) circuit is established between them…once set up, all communication between devices takes place over this circuit, even though there are other possible ways that data could conceivably be passed over the network of devices between them."[11]

A telephone network is an example of a circuit switching system. Here the problem of monitoring and attribution is simplified. "Whenever a connection between the parties involved is made, that communication can be monitored for the duration" of this established dedicated circuit.[12] Given the circuit is established a priori, the termination points and all routing (i.e. the entire dedicated path) in between is known and, thus, tracing back to the source of the transmission (level 1 attribution) can be simple. Figure 1 below shows the message, Hey, transiting from node A to node B via a notional routed path. Each rectangle along the path denotes a switch (router). The path highlighted denotes the circuit that remains dedicated for the duration of information passed between A and B.

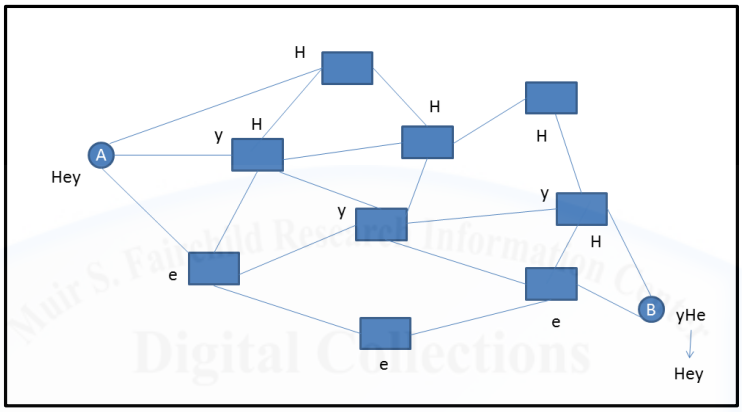
Figure 1. Circuit-Switched Network



The Internet can be described as a packet switching network versus other communications systems (e.g. analogue telephone voice communications) that utilize a circuit switching network. A packet switching network does not establish a path prior to transferring information between nodes. In this scheme, the information to be sent can be subdivided into packets and each packet can travel a different path to the final destination. "The packets can be routed, combined or fragmented, as required" and "on the receiving end, the process is reversed and the data is reassembled into the form of the original data."[13] Kozierok compares a packet-switched network to the postal system. Each post office can be thought of as a router on the network sending the letter (packet) to another post office (another router). Packets are sent without the nework knowing the entire route before hand. As a packet arrives at a post office (router), the next post office (router) is then decided upon. The process continues until the packet reaches the final destination.[14] Figure 2 shows the same message, Hey, sent from node A to node B via the packet-switched scheme where, notionally, each letter moves along a potentially different path, in a potentially differernt order in time and then rearranged to complete the message at node B. Each packet of data moves along an on-demand (versus dedicated) path throughout the length of time information is passed between A and B. Each new

piece of communication can be subdivided in a different fashion and take a different path depending on available recources on the network at that instant in time. As an advantage, a packet-switched network allows multiple users simultaneous use of a shared network since dedicated paths are not created for each communication instance as in a circuit-switched network.[15] However, intuitively, from this diagram, the problem of attribution in case of malicious intent begins to take shape.

Figure 2. Packet-Switched Network



Given the path is not known for the duration of the communication, can be fragmented across multiple changing paths and is spread across many routers throughout the network, each router would need to be monitored to filter out packets of interest with respect to communication between node A and B. Further, should A alter (spoof) his/her true source address or route packets through an intermediary computer, say C, attempts to trace back to the true source over a non-dedicated, on demand and multi-potential path scheme describes a much more complicated scenario than the dedicated path for the entire communication as was the case for a circuit switched network. Now that the general model for information transmission on the Internet has been described, a discussion of the protocols the Internet uses and the trusting context within which they were implemented will proceed.

Open Architecture and Transmission Control Protocol/Internet Protocol (TCP/IP)

ARPANET, the precursor to the Internet developed by DARPA, allowed communications between hosts on its network, but since its structure did not provide a communications architecture to allow other networks to connect to ARPANET, the current TCP/IP architecture was developed.[16] The original protocol, Network Control Protocol (NCP), did not have to manage any packet errors or lost packets since, at the time, ARPANET was the only network and its reliability was such that "no error control would be required on the part of the hosts."[17] Robert Kahn, who came to DARPA in 1972, introduced the notion of an open-architecture network. Specifically, an open-architecture system allows

> "multiple independent networks of rather arbitrary design…the choice of any individual network technology was not dictated by a particular network architecture but rather could be selected freely by a provider and made to interwork with other networks through a meta-level 'Internetworking Architecture'."[18]

TCP/IP provided this meta-level architecture via a communications protocol that the multiple indepentent networks would follow to establish communications. TCP/IP also dealt with packet errors, unlike NCP, by retransmitting packets that do not arrive and adding "end-end checksums, reassembly of packets from fragments and detection of duplicates" as well as flow control.[19] This added a level of reliability and robustness on a network of independent networks. In general IP provided addressing information (source and destination), while TCP provided the aformentioned management functions.

TCP/IP's lack of security as a consideration during its creation and its enabling of an open-architecure network of networks describes the main reasons complicating attribution today. TCP/IP was created within a trusted agent context since the community operating the early Internet was a "closed community of scholars."[20] Due to an atmosphere of trust, no check was

accomplished to verify the source and destination addresses in the IP address. Thus, an "attacker can alter them, known as IP spoofing" at will to obscure his/her true IP address and complicate knowlegde of his/her location and subsequent identification.[21] Further, no real management of the Internet exists at the operational level. The Internet transitioned from a U.S. government owned intranet to a patchwork of privately owned, independent networks.[22] Thus, the open-architecture structure of the Internet presents a myriad of networks contructed with different technology platforms and procedures within differing nations of different laws and regulations. Therefore, tracing an attacker back through this maze presents both technology hurdles, coordination/cooperation hurdles with differing Internet Service Providers (ISPs) and international legal and cooperation hurdles with other soveriegn states. Definitely TCP/IP provided a open environment to connect a network of networks to foster rapid innovation resulting in the benefits seen today, but an innovative open environment came at the expense of security. Having now provided a sufficient problem description and context surrounding attribution on the Internet, two different techniques to accomplish attribution will be discussed. These techniques by no means exhaust the space of possible ways to achieve attribution, but they provide good motivation to begin to argue that the problem of attribution is not the correct problem to solve.

Brief Survey of Two Techniques to Accomplish Attribution

IP Traceback via Router Log Storage

One technique to accomplish level 1 attribution (identification of the IP address of the machine involved in an attack) requires each router to keep a log of all packets that move through it. Thus, a defender can query each router one step from his/her computer to identify the next router an attack passed through to enable yet another query of every router connected to that

newly identified router. This process repeats to continue to move backwards toward the point of origin of the attacker.[23] Such an approach would require unlimited storage requirements at each router. To mitigate the storage issue and reduce privacy concerns, rather than storing the entire packet contents, only header information (for example source and destination) of the packet can be stored. Also, to prevent the issue of data being stored forever and eventually requiring more and more storage as well as computational resources over time, a time limit that data is held could be enforced (e.g. six months, a year, etc…).[24]

Three main issues with this approach prevent realistic implementation. First, to be effective worldwide, every country and private ISP would have to agree to implement router logging, a likely insurmountable requirement. Those ISPs/nations that do not participate would could be used attackers as intermediate transit points to prevent traceback beyond those locations that do not log packet header information. Second, even if implemented worldwide, such a system achieves only level 1 attribution. At best, for an attacker utilizing a multistage/multi-jurisdictional attack, one could identify the IP address of an innocent infected person's computer used unwittingly to mount the attack, but would not necessarily identity the controlling machine (level 2 attribution) nor the responsible party (level 3 attribution). Finally,

> "a defender would have to contact a wide set of ISPs, each with different policies and procedures, to request the logs. Since there is no standard implementation for storing logs, these logs would then have to be individually analyzed to retrieve the appropriate information."[25]

Even for an attacker who does not utilize a multistage attack, such an approach might still only achieve level 2 attribution due to "entry point anonymity."[26] An attacker can originate an attack from places such as cyber-cafes and public libraries where location of attack does not necessarily link to an individual perpetrator.[27]

Hack-Back

The hack-back technique involves infiltrating the actual machines in the chain involved in the attack vice just following the router chain. If an attacker exploited vulnerabilities in a "series of host machines", a defender can exploit those same vulnerabilities to insert a "host monitoring function" and identify the next machine backwards and so on of infected machines until reaching the attacker origin.[28] Such a technique provides an ability to move beyond level 1 attribution and achieving level 2 attribution (identifying attacker's computer) by infecting and monitoring the intermediate machines to identify the source controlling machine. Further, depending on the amount of personal data on the attacking machine, potentially level 3 attribution could be achieved. However, especially within the United States, actual infiltration and monitoring of machines represents violations of privacy and constitutes search and seizure. Thus, the technique would require a legal warrant, potentially, for each intermediary machine infiltration.[29] In the event an attack is large enough to represent a national security issue (e.g. attack severely disrupting DOD networks or financial/banking infrastructure) "one may expect such techniques to be employed" and privacy concerns superseded by the level of the threat and warrant needs expeditiously granted.[30] However, a sophisticated attacker may attempt to eliminate those same vulnerabilities that enable a hack-back, in essence hardening the intermediate machines complicating the defender's attempts to hack back. Further, some hack-backs must be accomplished before the attack stops adding a time constraint to the process.[31]

These two examples of technical solutions to accomplish attribution exemplify the asymmetric capability and resource gap between the attacker and the defender. The capabilities and resources needed for an attacker to obscure his/her identity pale in comparison to those needed by the defender to identify the attacker. Lack of international cooperation, multiple

jurisdictions, lack of standardized network configurations (such as router logging), inability to enforce those standards globally and technical countermeasures that must be implemented under time constraints characterize part of the asymmetric disadvantages a defender must overcome. An attacker need only gain entry at an anonymous point and/or infect intermediate computers within multiple jurisdictions to shroud him/herself, frustrate investigation cooperation and launch attacks. Notwithstanding the technical hurdles, do policy options provide a means to level the battlefield between attacker and defender with respect to solving attribution to enable deterrence? Policy choices will now be investigated to determine if a feasible, implementable solution exists.

Policy Response Options for Attribution

Robert K. Knake (director for Cybersecurity Policy in the US National Security Council 2011-2015) and Martin C. Libicki (senior management scientist, RAND) offer a similar viewpoint on creating international norms of behavior in cyberspace but differ on accountability policy. This paper stipulates as an assumption that creating international norms constitutes an element of the long term strategy for increased trust and strategic stability in cyberspace. Thus, this section will rather focus on where these policy professionals disagree on accountability policy to highlight the consequences and continue to advance an argument against overly focused efforts on just attribution to achieve deterrence via retaliation.

Hold Intermediaries Accountable

For both high-end attacks (e.g. cyber war) and medium-end (e.g. cyber crime) Knake argues that the U.S. should "move beyond the search for perfect attribution and instead hold states that do not cooperate accountable."[32] Here perfect attribution can be inferred to mean level 4 attribution as defined on page 3, the identification of the higher organization with a specific purpose for the attack. Specifically, Knake describes no longer treating "intermediary

systems as victims and start viewing them as accomplices…and make a public position that treats failure to cooperate in investigating a cyber attack as culpability."[33] Knake attempts to simplify the attribution problem of multi-stage/muti-jurisdictional attacks by recommending the U.S. achieve level 1 attribution first (identification of specific intermediary machines involved in a multistage attack) and then relying on tools of statecraft (if outside the U.S.), namely threats of retaliation, to force cooperation and allow continued investigation to identify the true source of the attack. Further, this policy position intends to create incentives (albeit via negative punishment) for states not only to cooperate in investigations, but also work to secure their cyber infrastructure.[34] On the surface such a policy prescription sounds appealing with regard to providing a discrete course of action, imparting costs on intermediaries and, theoretically, changing the cost/risk/benefit calculation of an attacker. However, an analysis of second order effects reveals the folly of such a policy.

Denial & Resiliency

Such a cavalier policy as holding non-cooperative intermediaries accountable leads to undesirable crisis enlargement/escalation and incentivizing false-flag operations. If the U.S. makes such a public policy declaration, it amounts to a declarative redline for action. Such declarative redlines incentivize states' interests in manipulating America's responses. Specifically, Libicki states that severe threats of retaliation on non-cooperative intermediaries raise the probability that attackers choose an intermediary state that has similar motives for attacking the U.S. as well as high likelihood for being non-cooperative, thus, making the state appear guilty (i.e. false-flag operations).[35] This could be the case not only for attackers outside the U.S. but even ones inside the U.S. Furthermore, such a policy has the effect of creating instability by leading to potential enlargement of the crisis by creating unnecessary escalation

with multiple third parties. Also, Knake's policy suggestion attempting to incentivize nations to secure their cyber space such that they can prevent being used as an intermediary assumes this is even possible. Even the U.S., arguably with the one of the most modern internet infrastructures, was unable to prevent being the staging ground for one-sixth of all internet attack traffic directed against Estonia from Russia in 2007.[36] The ambiguity of actions in cyberspace (both who did it and for what purpose) plus potential knee-jerk reactions to retaliate combine to provide an increased likelihood of miscalculations and instability. Libicki delivers the best policy argument in such an environment. He states that crisis stability requires demonstrating and communicating the ability to continue to operate in the face of cyber attack.[37] Thus, the focus is less on attribution and more on denial of benefits via defense and resilience to achieve deterrence. But how can a meaningful defense be achieved where the asymmetric advantages favor the offense? Why not turn the asymmetric advantages that favor the offense on its head and make them the advantages of the defense? The following sections make such an argument.

Attribution or Denial Focus, Asymmetric Advantage of Attacker Problem

So far this paper has provided evidence of the asymmetric complexity of the attribution problem from the perspective of the defender compared to the attacker from both a technological and policy standpoint. The cost and complexity faced by the attacker to shroud his/her identity is comparatively small compared to the defender's attempts to identify the attacker and retaliate to create deterrence as described in the previous sections. The attacker simply relies on redirecting attacks from intermediary computers and/or gaining entry into a network from an anonymous point (cyber café, library or the like). The attacker creates a multi-jurisdictional, multi-stage distance between his/her identity/location and the IP address of the machine accomplishing the attack. The defender faces a fog of misdirection and attack approaches from multiple directions

where technical solutions can require mass changes to the Internet infrastructure (as seen from the router logging discussion) and policies of retribution to intermediaries (as Knake prescribes) that can likely create instability and chaos which may be exactly the confusion an attacker may wish to create.

In response to such an environment the United State Air Force (USAF) sought to centralize access to its unclassified networks by reducing the number of gateways from the 100s to 16.[38] The USAF describes the move as enabling "centralized defense, operation and management of the Air Force Network Enterprise."[39] Some state this makes active monitoring of the networks to detect intrusions easier as well as standardize configurations for ease of active monitoring management.[40] From the standpoint of the attacker, this defender (USAF) creates a uniform, discrete and static beachhead (16 static gateways) to attack and once any vulnerability is discovered it can be exploited for the entire system (due to standard configurations). This strategy exemplifies early industrial age Maginot Line notions of centralization and hardening against an information age, mobile threat. It defines an anachronistic strategy just as the French created with the Maginot Line postured against blitzkrieg mobile warfare fought by the Germans in World War II. Had World War II consisted of trench positional warfare that defined World War I, perhaps the Maginot Line might have been successful. The strategy taken by the Air Force could also be deemed as positional warfare…static gateways, centralized and hardened. The strategy fails to take advantage of the one aspect of the cyber domain that distinguishes it from the air, land, space and sea domains. The cyber domain can be recreated at will and changed. Man writes the rules in this domain.

Perhaps solving the attribution problem is the wrong problem given its intractable nature and asymmetric advantage it provides the attacker. Rather than positional warfare as being

practiced by the USAF, why not engage in maneuver warfare in cyberspace from the perspective of the defender? Those capability attributes that create cost and complexity for the defender can be redirected against the attacker. Could anonymity and misdirection via creating a shifting multi-platform front complicate an attacker's efforts to identify and attack those networks of the defender? Could deterrence be better enabled with a higher focus on denial of benefits via raising attacker's cost and complexity to conduct attacks? Definitely the threat of retaliation comprises a portion of the deterrence equation. However, for deterrence to be effective in cyberspace, a more effective and sustainable defense that creates more opportunities to deny benefits to the attacker is needed. The next section provides an example of rethinking defense to accomplish such a rebalance of the asymmetric advantages enjoyed by the attacker toward the defender. Stability can be achieved when more symmetry exists between resources and effectiveness in the comparison of offense and defense.

Denial through Complicating the Attack Surface, Increasing Attacker Costs

This section will review a moving target defense strategy that defines its network via software (logical algorithm) instead of physical static gateways. By no means does this paper argue that this technical approach represents a panacea solving the deterrence problem via complete denial of benefits to the attacker in cyberspace. Rather, a discussion of such an approach exemplifies the type of transformational thinking that uses the unique qualities of the cyber domain to a defender's advantage. Namely, it takes advantage of the ability to recreate the domain at will and moves cyberspace security from a positional to a maneuver based defense.

Jafarian, Al-Shaer and Duan in the Department of Software and Information Systems at the University of North Carolina (UNC) at Charlotte propose a method of random host mutation, i.e. changing the IP addresses of end-hosts both frequently and randomly. They argue that "static

configurations" and "static assignment of IP addresses gives adversaries significant advantage to remotely scan networks and identify their targets accurately and quickly."[41] This identification of "active IP addresses in a target domain is a precursory step for many attacks."[42] The system they propose keeps the original IP addresses of the actual hosts on the network, but creates a mapping of each real host with a random "short-lived virtual IP address" taken from the "unused address space of the network."[43] Subnet gateways perform the real IP to virtual IP translation and a network controller "coordinates the mutation rate across the network."[44] Such a system would give network administrators ability to still monitor their real, unchanged hosts/gateways. However, it creates a random, mutating front of unpredictable virtual IP addresses to misdirect an attacker and provide anonymity by shrouding the defenders true network behind a fog of moving virtual hosts. This type of thinking creates an ever changing attack surface rather than the static beachhead created by current USAF unclassified network architecture. These researchers at UNC Charlotte constructed and tested their network and results reduced the accuracy of an attacker's network scanning up to 99% and scanning worms were unable to infect 90% of the real network hosts.[45]

Proposals such as this create meaningful layered defenses by reducing the throughput of successful attacks and, potentially, lowering resources the defender devotes to responding to successful attacks. Similarly, Zheng at Texas Tech University recommends system diversity, i.e. we should "dynamically change system configurations to add uncertainty, unpredictability and diversity" to our networks so that "the system is unpredictable to attackers, hard to be exploited and is more resilient to attacks."[46] These proposals increase costs and shift the same complexity issues seen in the attribution problem on the attacker. The U.S. government and the USAF (the cyber force bearer of the U.S.) should investigate implementing such maneuver based defensive

approaches and move away from its anachronistic positional warfare cyber strategy as seen in the Air Force network architecture.

Conclusion

Efforts to solve the attribution problem via technological means and/or policy means describe a never ending death spiral of potential resource exhaustion and potential overreaction/miscalculation leading to instability. Making global changes to the Internet to improve monitoring (the router logging solution as an example) still does not solve the attribution problem created by multi-stage, multi-jurisdictional attacks. Hack-backs are time constrained and assume defenders can exploit the same vulnerabilities the attacker used to gain access to intermediary machines. Policies that recommend holding intermediary states (where attacks transit) accountable incentivizes false-flag operations by the attacker and risks unnecessary enlargement of the conflict to multiple third parties. Such thinking could lead to miscalculation and chaos an attacker wishes to create. As Libicki notes, presenting a credible front of resiliency in the face of cyber attack represents a more level headed policy approach communicating to would-be attackers they will not gain the benefits they seek. The truly clever technical approaches to achieve resiliency take those capabilities that give the attacker asymmetric advantages (namely anonymity, ambiguity and mobility) and coopt them for the defender. Constantly changing the defender's attack surface via randomly mutating IP addresses and dynamically changing system configurations moves the cyber security strategy out of the industrial age and into the information age. Transformational strategies to achieve cyber deterrence must take advantage of the fundamental difference of the cyber domain as the one domain that can be manipulated and recreated at will. The problem isn't attribution, it's our defense strategy.

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. Clark and Landau, "Untangling Attribution", 25-26.
2. Cohen and Narayanaswamy, *Survey/Analysis of Levels I, II and III Attack Attribution Techniques,* 4.
3. Knake, "Untangling Attribution: Moving to Accountability in Cyberspace," 3.
4. Ibid., 3.
5. Ibid., 3.
6. Ibid., 4.
7. Yannakogeorgos, *Strategies for Resolving the Cyber Attribution Challenge,* 14
8. Yannakogeorgos, *Strategies for Resolving the Cyber Attribution Challenge,* 14 and Clark and Landau, "Untangling Attribution", 31.
9. Yannakogeorgos, *Strategies for Resolving the Cyber Attribution Challenge,* 5 and Knake, "Untangling Attribution: Moving to Accountability in Cyberspace," 7.
10. Clark and Landau, "Untangling Attribution", 31-33; Yannakogeorgos, *Strategies for Resolving the Cyber Attribution Challenge,* xvii; Knake, "Untangling Attribution: Moving to Accountability in Cyberspace", 7-8.
11. Kozierok, *Circuit Switching and Packet Switching Networks*
12. Kantzer, Cyber Attack Attribution, 20.
13. Kozierok, *Circuit Switching and Packet Switching Networks*
14. Kantzer, Cyber Attack Attribution, 19.
15. Ibid., 19-20.
16. Ibid., 20-21.
17. Leiner, "Brief History of the Internet", 4.
18. Ibid., 3.
19. Ibid., 4.
20. Kantzer, Cyber Attack Attribution, 22.
21. Ibid., 22-23.
22. Ibid., 33.
23. Wheeler and Larsen, "Techqniques for Cyber Attack Attribution", 11.
24. Kantzer, *Cyber Attack Attribution,* 56.
25. Kantzer, *Cyber Attack Attribution,* 58.
26. Hunker, Hutchinson and Marguilies, *Roles and Challenges for Sufficient Cyber-Attack Attribution,* 15.
27. Ibid., 15.
28. Ibid., 19.
29. Kantzer, *Cyber Attack Attribution,* 72.
30. Ibid., 73.
31. Ibid., 74.
32. Knake, "Untangling Attribution: Moving to Accountability in Cyberspace," 8.
33. Ibid., 7-8.
34. Ibid., 7.
35. Libicki, *Cyber Deterrence and Cyber War,* 44.
36. Libicki, *Crisis and Escalation in Cyberspace,* 24.
37. Ibid., 148.
38. Stoner, "Architecture Way Ahead", slide 15.
39. Ibid., 15.
40. Lecture, ACSC.
41. Jafarian, Al-Shaer, and Duan. *Open Flow Random Host Mutation: Transparent Moving Target Defense*, 127.
42. Ibid., 127.
43. Ibid., 127.
44. Ibid., 127.
45. Ibid., 128.
46. Zheng, *Moving Target Defense in Cyber Security,* slide 7.

Bibliography

Clark, David D., and Susan Landau. "The Problem isn't Attribution, It's Multi-Stage Attacks." *Privacy Ink.* November 2010. http://www.privacyink.org/pdf/Clark_Landau_ReArch10.pdf (accessed March 20, 2015).

—. "Untangling Attribution." *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy.* Washington, DC: The National Academies Press, 2010. 25-40. http://cs.brown.edu/courses/csci1950-p/sources/lec12/ClarkandLandau.pdf (accessed 17 Jan 2015).

Cohen, Don, and K. Narayanaswamy. *Survey/Analysis of Levels I, II, and III Attack Attribution Techniques.* Research Project Sponored by Advanced Research and Development Activity (ARDA), Los Angeles: CS3 Inc., 2004. http://www.scis.nova.edu/~cannady/ARES/cohen.pdf (accessed 16 Feb 2015).

Hunker, Dr. Jeffrey, Jeffrey Hutchinson, and Jonathan Margulies. *Roles and Challenges for Sufficient Cyber-Attack Attribution.* Whitepaper, Hanover: Institute for Information Infrastructure Protection, Dartmouth College, 2008. http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf (acessed 14 Jan 2015).

Jafarian, Jafar Haadi, Ehab Al-Shaer, and Qi Duan. *Open Flow Random Host Mutation: Transparent Moving Target Defense unsing Software Defined Networking.* University of North Carolina at Charlotte, Department of Software and Information Systems. August 13, 2012. https://www.ece.cmu.edu/~ece739/papers/movingtarget.pdf (accessed February 25, 2015).

Kantzer, Kenneth Han-Wei. *Cyber Attack Attribution: An Asymmentrical Risk to U.S. National Security.* Senior Thesis, Princeton: Princeton University, 2011. https://www.pkcsecurity.com/data/Cyber_Attack_Attribution.pdf (acessed 10 Feb 2015).

Knake, Robert K., "Untangling Attribution: Moving to Accountability in Cyberspace," Testimony before United States House of Representatives, 2nd Session, 111th Congress, Subcommittee on Technology and Innovation, Committee on Science and Technology. July 15, 2010. http://www.cfr.org/united-states/untangling-attribution-moving-accountability-cyberspace/p22630 (accessed 14 Jan 2015).

Kozierok, Charles M. *The TCP/IP Guide.* September 20, 2005. http://www.tcpipguide.com/free/t_CircuitSwitchingandPacketSwitchingNetworks.htm (accessed February 16, 2015).

Leiner, Barry M., et al. "Brief History of the Internet." *Internet Society.* October 15, 2012. http://www.internetsociety.org/brief-history-internet (accessed March 22, 2015).

Libicki, Martin C. *Crisis and Escalation in Cyberspace.* Monograph, Arlington: RAND Corporation, 2012.

Libicki, Martin C. *Cyber Deterrence and Cyber War.* Monograph, Arlington: RAND Corporation, 2009.

Stoner, Steve. "Architecture Way Ahead." Air Force Network Integration Center. September 19, 2012. www.afnic.af.mil/shared/media/document/AFD-120919-056.pdf (accessed April 6, 2015).

Wheeler, David A., and Gregory N. Larsen. "Techqniques for Cyber Attack Attribution." *Institute for Defense Analysis.* October 2003. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859 (accessed February 10, 2015).

Yannakogeorgos, Panayotis A. *Strategies for Resolving the Cyber Attribution Challange.* Maxwell Air Force Base: Air University Press, 2013.

Zheng, Jianjun. "Texas Tech University, Department of Computer Science, Summer Workshop on Cyber Security." *Moving Target Defense in Cyber Security.* July 2014. www.depts.ttu.edu/cs/research/csecs/workshop/docs/2014/keynote/MTD-Overview.pptx (accessed March 21, 2015).